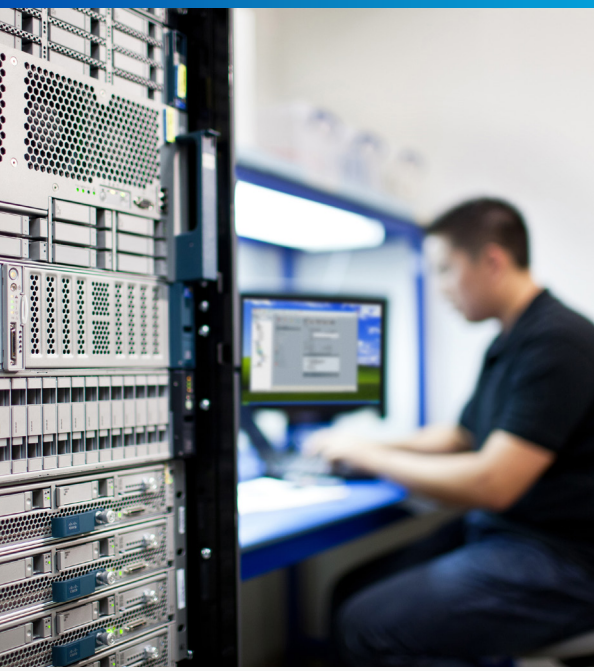
Threat Management



Benefits

- Stronger security posture through a comprehensive approach that addresses both readiness and response
- Higher confidence in ongoing protections through a proven methodology, unique intelligence, and an experienced team
- Greater visibility and deeper understanding of your operations and infrastructure through the use of innovative technology and extensive ongoing analysis by experts

Cisco Security Advisory Services
Incident Response

Organizations are under attack everywhere. In 2014, security breaches cost nearly $500 billion, according to IDC. Meanwhile there's a worldwide shortage of security professionals, with an estimated one million openings going unfilled, according to the Cisco 2015 Annual Security Report.

Today's Dynamic Threat Landscape

This talent shortage, combined with an increase in incidents, has led to a generally weak security posture among most organizations. Successful attacks result in huge monetary losses, lost intellectual property, compromised client information and confidence, and lower corporate valuations.

The Cisco® Security Incident Response Service significantly strengthens your network and information security defenses. Using the latest intelligence and best practices, it introduces a process that engages all layers of defense and provides a comprehensive range of capabilities to help organizations prepare, manage, respond to, and recover from incidents quickly and effectively.

Only 50% of CISOs strongly agree "It is easy to determine the scope of a compromise, contain it, and remediate from exploits"

—Cisco Annual Security Report 2015

Stronger Security Posture with Readiness and Response

The Cisco® Security Incident Response Service is a solution within Cisco Advisory Security Services that provides the expertise to assess and design a security approach that fosters business growth, reduces cost, and mitigates risk. By synthesizing best practices and utilizing effective industry security frameworks, Cisco's Incident Response Team provides a comprehensive range of capabilities to help organizations. Our Incident Response Team consists of information security experts with a unique blend of law enforcement, enterprise security, and technology security backgrounds. Our team works directly with the Collective Security Intelligence (CSI) Group to identify known and unknown threats, quantify and prioritize risk, and reduce risk in the future.

Let our experts work with you to develop a new plan, revaluate existing plans, or provide rapid assistance in the midst of attack.

Cisco Security Advisory Services: Incident Response

Readiness: Proactive Services

- **Infrastructure Breach Preparedness Assessment:** By evaluating network design, security controls, operating systems, personnel security configuration, automated patching systems, firewalls, logging, and other related systems, Cisco obtains a deep understanding of the client's environment and is able to predict potential attack vectors and recommend necessary security controls.
- **Security Operations Readiness Assessment:** Through an assessment of your security team's readiness, based on prior incidents and current roles and responsibilities, Cisco provides recommendations on whether your organization has the necessary resources, knowledge, and tools for various types of investigations.
- **Operations Readiness Assessment:** Recommendations to help with future events are provided through an assessment of your operations model and activities.
- **Breach Communications Assessment:** Cisco provides assistance with building a communications framework with an appropriate compliance structure for coordinated awareness and response at the board level, across the organization's supply chain, and externally with clients.
- **Security Operations and Incident Response Training:** Training is given on the latest skills needed to lead, coordinate, and support an incident. In addition, technical training is offered to security operations personnel for malware analysis and various security tools.

Response: Reactive Services

- **Evaluation and Investigation:** Determines the method of attack and pulls together a breakdown of the malicious code, including its trajectory, destination, and end goal, through a technical review of the infected system(s).
- **Countermeasure Development:** Develops countermeasures to aid in detecting, quarantining, tracking, and stopping further actions by the attacker. These may produce indicators of compromise, information leakage, and vulnerability exploitation.
- **Countermeasure Deployment:** Deploys all countermeasures that have been developed to aid in detecting and stopping the incident, all done in accordance with information security and vendor best practices.
- **Countermeasure Validation:** Validates the effectiveness of newly deployed countermeasures and compiles a performance review of any needed enhancements to the design. The output includes documentation for the boardroom, regulatory bodies, and law enforcement detailing the event summary, mitigation, and loss if applicable.

Cisco's incident response may include any or all of the following to isolate and remediate an attack:

- Log source assessment
- Analysis and data mining
- Forensic image analysis
- Infected system dynamic instrumentation
- Malware reverse engineering
- Exploit analysis and re-implementation

Case Study

Case Study: Retail Company

Challenge

Client experienced a breach, they lacked security experts to respond to advanced threats and infrastructure failed to block malware.

Solution

During a seven-day engagement, Cisco provided custom malware detection capabilities through network forensics, malware sample analysis, malware countermeasure development, network anomaly detection, and a comprehensive review of intelligence.

Outcome

- Provided data to create a solid security posture, as related to both endpoint malware, data in transit, and the overall communication capabilities within the infrastructure.
- Located numerous types of commodity malware within the infrastructure that the client's traditional AV solutions were not capturing.
- Increased visibility into network, utilizing the solutions that revealed security deficiencies, misconfigurations, application shortcomings (as related to security).

Next Steps

Visit www.cisco.com/go/securityservices to connect with our advisors and protect your business today.

DEC14CS4667 07/15